Foreman - Bug #19169
CVE-2017-2672 - audit trail leaks sensitive data for Image events
04/04/2017 03:57 PM - Daniel Kimsey

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Marek Hulán</td>
</tr>
<tr>
<td>Category:</td>
<td>Audit Log</td>
</tr>
<tr>
<td>Target version:</td>
<td>1.15.0</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman/pull/4438">https://github.com/theforeman/foreman/pull/4438</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td></td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>1447510</td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td>1.13.4</td>
</tr>
</tbody>
</table>

**Description**

If one looks at an audit record for Image creation, the password used is recorded in plaintext. This must be censored.

The attached image is rendered from a specific audit entry, such as: [https://katello.acme.com/audits/1234](https://katello.acme.com/audits/1234)

**Related issues:**

Related to Foreman - Refactor #20116: Redact sensitive information from audit... New 06/27/2017
Related to Foreman - Refactor #21920: Refactor password auditing Closed 12/10/2017

**Associated revisions**

Revision 02489389 - 04/06/2017 05:16 AM - Marek Hulán
Fixes #19169 - remove image password from audit

Revision bae2fa2b - 04/24/2017 09:58 AM - Marek Hulán
Fixes #19169 - remove image password from audit

**History**

#1 - 04/05/2017 02:48 AM - Marek Hulán
- Category changed from Web Interface to Audit Log

#2 - 04/05/2017 03:17 AM - The Foreman Bot
- Status changed from New to Ready For Testing
- Assignee set to Marek Hulán
- Pull request https://github.com/theforeman/foreman/pull/4438 added

#3 - 04/06/2017 04:04 AM - Dominic Cleal
- Subject changed from audit trail leaks sensitive data for Image events to CVE-2017-2672 - audit trail leaks sensitive data for Image events

Report forwarded to foreman-security@googlegroups.com, CVE-2017-2672 was assigned to identify the vulnerability.

#4 - 04/06/2017 05:44 AM - Marek Hulán
- Target version set to 1.13.0

#5 - 04/06/2017 06:01 AM - Marek Hulán
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100
Applied in changeset 02489389f1a4443e1f437b86aa7ce245f1437020.

#6 - 04/11/2017 04:23 AM - Daniel Lobato Garcia
   - Legacy Backlogs Release (now unused) set to 209

   Setting to 1.15, it'll be cherry-picked for RC2.

#7 - 05/11/2017 01:51 PM - Bryan Kearney
   - Bugzilla link set to 1447510

#8 - 06/27/2017 04:45 AM - Tomer Brisker
   - Related to Refactor #20116: Redact sensitive information from audit logs added

#9 - 12/10/2017 03:47 PM - Michael Moll
   - Related to Refactor #21920: Refactor password auditing added

Files
Screen_Shot_2017-04-04_at_14_43_36.png      37.8 KB      04/04/2017      Daniel Kimsey